Summer Research Proposal:
Marrying Gradual and Linear Types
The Attack Tree Linear Logic (ATLL)

Harley Eades III, Computer Science, Augusta University

1 Overview

This proposal seeks summer faculty salary support from the Hull College of Business for the months of June and July to support two cutting edge research projects in computer science and cyber security. I briefly describe these projects before discussing the summer activities that the requested funds will support.

2 Marrying Gradual and Linear Types

Gradual typing is a new area of research in the theory of programming languages that impacts much of the technical industry. Linear types provide a means of specifying and broadening computer programs to be more safe when dealing with input from the outside world. This project will be the first to bring these two paradigms together providing the best of both worlds.

Over the course of the summer my trainee, a Ph.D. student from the University of Iowa, and I will develop a new programming language that combines gradual and linear types. We will then mathematically prove the correctness of this programming language inside a new cutting edge system called Agda which is a proof assistant for conducting machine checked mathematical proofs. This will certify that our programming language meets all of the desired properties solidifying its correctness.

3 The Attack Tree Linear Logic (ATLL)

Attack trees are a modeling tool, originally proposed by Bruce Schneier [3], which are used to assess the threat potential of a security critical system. Attack trees have since been used to analyze the threat potential of many types of security critical systems, for example, cybersecurity of power grids [4], wireless networks [2], and many others. Attack trees consists of several goals, usually specified in English prose, for example, “compromise safe” or “obtain administrative privileges”, where the root is the ultimate goal of the attack and each node coming off of the root is a refinement of the main goal into a subgoal. Then each subgoal can be further refined. The leaves of an attack tree make up the set of base attacks. Subgoals can be either disjunctively or conjunctively combined.

The need for a foundation. Attack trees for real-world security scenarios can grow to be quite complex. The attack tree presented in [4] to access the security of power grids has twenty-nine nodes with sixty counter measures attached to the nodes throughout the tree. The details of the tree spans several pages of appendix. The attack tree developed for the border gateway protocol has over a hundred nodes [1], and the details of the tree spans ten pages. Manipulating such large trees without a formal semantics can be dangerous.

The formal semantics of attack trees. The leading question the field is seeking to answer by giving a mathematical foundation to attack trees is "what is an attack tree?" There have been numerous attempts at answering this question. However, the research on the mathematical foundation of attack trees being done here at Augusta University[1] is the first of its kind, and the first to propose the use of linear logic.

This summer my trainee, a visiting Ph.D. student from North Carolina State University, will aid me in developing a new system for reasoning about attack trees and conducting threat analysis using attack trees called the Attack Tree Linear Logic (ATLL). This system is the first of its kind and has the potential to greatly impact the cyber security research community.

4 The Proposal

I will be hosting two visiting Ph.D. students from June 1 till Augusta 1. They will be fully funded from my NSF grant, fn. 1, but this grant does not include PI salary support.

The amount I am requesting is $10,000. This will cover my salary for the summer months of June and July. The amount of effort required for the proper mentorship and research development necessary for this summer is at least as much effort as teaching a summer course. Lastly, this research program benefits, not only myself, but the college and university as a whole, because I will be mentoring two visiting Ph.D. students as well as building relationships with other universities through this mentorship.

In addition, I will be holding a summer research seminar that will be open to Hull College of Business students as well as three graduate students and two postdocs from the University of Iowa. The project will begin on June 1 and end on July 30.

At the completion of the summer project I will happily provide drafts of the two papers these projects will produce to the college and/or present the results and activities to the college during a brown bag.

References

[1] S. Convery, D. Cook, and M. Franz. An attack tree for the border gateway protocol. 2003. `https://tools.ietf.org/html/draft-ietf-rpsec-bgpattack-00`.

[2] A. Reinhardt, D. Seither, A. Konig, R. Steinmetz, and M. Hollick. Protecting ieee 802.11s wireless mesh networks against insider attacks. In *Local Computer Networks (LCN), 2012 IEEE 37th Conference on*, pages 224–227, Oct 2012.

[3] Bruce Schneier. Attack trees: Modeling security threats. *Dr. Dobb's journal*, December 1999.

[4] Chee-Wooi Ten, Chen-Ching Liu, and Manimaran Govindarasu. Vulnerability assessment of cybersecurity for scada systems using attack trees. In *Power Engineering Society General Meeting, 2007. IEEE*, pages 1–8, June 2007.

[1] The National Science Foundation CRII CISE Research Initiation grant, "CRII:SHF: A New Foundation for Attack Trees Based on Monoidal Categories", under Grant No. 1565557.